IN THE CLAIMS

Please amend claims 1, 7, 16, 21, 25, and 26 as indicated below.

This listing of claims will replace all versions, and listings, of claims in the application.

Listing of Claims:

Claim 1 (currently amended) A method comprising the steps of:

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);

creating, by a processor, a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

Claim 2 (original) The method as recited in claim 1, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.

Claim 3 (original) The method as recited in claim 1, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.

Claim 4 (original) The method as recited in claim 1, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

Claim 5 (original) The method as recited in claim 4, wherein the third certificate is associated with an endorsement key of the TPM.

Claim 6 (original) The method as recited in claim 1, wherein the network is the Internet.

Claim 7 (currently amended) A method comprising the steps of:

creating a TPM identity at a customer's computer system;

obtaining, at the customer's computer system, a first certificate from a first server supporting a CA over a network;

creating, by a processor at the customer's computer system, a non-migratable key; and

transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company.

Claim 8 (original) The method as recited in claim 7, further comprising the steps of:

the second server supporting the credit card company creating a public/private key pair and a second certificate in response to the transferring step; and

transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system.

Claim 9 (original) The method as recited in claim 8, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using a traditional mail service.

Claim 10 (original) The method as recited in claim 8, wherein the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system is performed using the network.

Claim 11 (original) The method as recited in claim 8, further comprising the step of:

a customer using the public/private key pair and the second certificate for commercial transactions over the network.

Claim 12 (original) The method as recited in claim 11, wherein the network is the Internet.

Claim 13 (previously presented) The method as recited in claim 7 further comprising the step of:

creating a public/private key pair.

Claim 14 (original) The method as recited in claim 13, wherein the step of the customer's computer system obtaining the first certificate from the first server supporting the CA over the network further comprises the steps of:

transferring from the customer's computer system to the first server supporting the CA a public portion of the public/private key pair created when the TPM identity is created and a third certificate associated with an endorsement key of the TPM;

the CA checking an authenticity of the third certificate;

the CA creating a fourth certificate for the TPM identity;

the CA encrypting the fourth certificate;

the CA bundling the encrypted fourth certificate with the public portion of the public/private key pair created when the TPM identity is created to create a first bundle; and

the CA encrypting the first bundle with a public key of the third certificate to create a second bundle.

Claim 15 (previously presented) The method as recited in claim 14 further comprising the step of:

transferring the public/private key pair and a second certificate from the second server supporting the credit card company to the customer's computer system further comprises the steps of:

the TPM decrypting the second bundle with a private portion of the third certificate producing the first bundle; and

the TPM decrypting the first bundle with a private portion of the public/private key pair created when the TPM identity is created.

Claim 16 (currently amended) A computer program product ~~adaptable for storage on~~ embodied in a computer readable storage medium, comprising the program steps of:

receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);

creating a public/private key pair and a third certificate in response to the receiving step; and

sending the public/private key pair and the third certificate to the customer over the network.

Claim 17 (original) The computer program product as recited in claim 16, wherein after the sending step, the customer is capable of using the public/private key pair and the third certificate to make purchases over the network.

Claim 18 (original) The computer program product as recited in claim 16, wherein the TPM identity is a public/private key pair created as a result of a command by the customer input into the computer system.

Claim 19 (original) The computer program product as recited in claim 16, wherein the second certificate is created by the Certification Authority in response to receiving a third certificate signed by a manufacturer of the TPM and a public key of the TPM identity.

Claim 20 (original) The computer program product as recited in claim 19, wherein the third certificate is associated with an endorsement key of the TPM.

Claim 21 (currently amended) A computer program product ~~adaptable for storage on~~ embodied in a computer readable storage medium, comprising the program steps of:

creating a TPM identity;

obtaining a first certificate from a CA;

creating a non-migratable key;

contacting a web site supporting a credit card company;

sending to the web site an application for a credit card authorization, the TPM identity, the first certificate, and the non-migratable key; and

receiving from the web site a public/private key pair and a second certificate enabling the credit card authorization.

Claim 22 (original) The computer program product as recited in claim 21, further comprising the program step of:

conducting a commercial transaction over the Internet using the credit card authorization as enabled by the public/private key pair and the second certificate.

Claim 23 (original) The computer program product as recited in claim 21, wherein the non-migratable key is a signing key.

Claim 24 (original) The computer program product as recited in claim 21, wherein the non-migratable key is a storage key.

Claim 25 (currently amended) A system comprising:

a server supporting a web site of a credit card company;

a customer computer including a TPM; and

a network linked to the server and the customer computer;

wherein the customer computer comprises a memory, wherein a first software is stored in the memory in the customer computer for requesting the TPM to create a TPM identity[[;]], wherein a second software is stored in the memory in the customer computer for obtaining a first certificate over the network from a CA[[;]], wherein a third software is stored in the memory in the customer computer for creating a non-migratable key[[;]], wherein a fourth software is stored in the memory in the customer computer for browsing the web site of the credit card company over the network[[;]], wherein a fifth software is stored in the memory in the customer computer for sending an application for a credit card authorization to the web site of the credit card company over the network[[;]], wherein a sixth software is stored in the memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key;

wherein the web site of the credit card company ~~creating~~ creates a public/private key pair and a second certificate; and

wherein the web site of the credit card company ~~sending~~ sends the public/private key pair and the second certificate over the network to the customer computer.

Claim 26 (currently amended) A system comprising:

a memory[[;]], wherein code is stored in said memory;

~~code stored in said memory;~~

an adapter which communicates data to and receives data from a certificate server and a credit card application server;

a Trusted Platform Module (TPM);

a CPU, operatively coupled to said memory, said TPM, and said communications adapter, and which executes code stored in said memory;

said CPU when executing said code effective in:

creating a TPM identity;

obtaining from said communications adapter a first certificate originating from said certificate server;

creating a non-migratable key; and

transferring a credit card authorization application, said TPM identity, said non-migratable key, and said first certificate to said credit card application server.

Claim 27 (original) Apparatus comprising:

an adapter through which data is exchanged with a certificate server and a credit card application server, a Trusted Platform Module (TPM) which creates a TPM identity; a CPU coupled to said adapter and to said TPM and effective in:

(1) obtaining from said adapter a first certificate originating from the certificate server;

(2) creating a non-migratable key and transferring said non-migratable key, said TPM identity, said first certificate, and a credit card authorization application to the credit card application server.